



# FortiAnalyzer v5.0.7 Upgrade Guide



## FortiAnalyzer v5.0.7 Upgrade Guide

June 27, 2014

05-507-245305-20140627

Copyright© 2014 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

|                            |  |
|----------------------------|--|
| Fortinet Document Library  | <a href="http://docs.fortinet.com">docs.fortinet.com</a>         |
| Fortinet Video Library     | <a href="http://video.fortinet.com">video.fortinet.com</a>       |
| Fortinet Knowledge Base    | <a href="http://kb.fortinet.com">kb.fortinet.com</a>             |
| Customer Service & Support | <a href="http://support.fortinet.com">support.fortinet.com</a>   |
| Training Services          | <a href="http://training.fortinet.com">training.fortinet.com</a> |
| FortiGuard                 | <a href="http://fortiguard.com">fortiguard.com</a>               |
| Document Feedback          | <a href="mailto:techdocs@fortinet.com">techdocs@fortinet.com</a> |

# Table of Contents

|  |           |
|--|-----------|
| <b>Change Log .....</b>                              | <b>4</b>  |
| <b>FortiAnalyzer Firmware.....</b>                   | <b>5</b>  |
| Best practices .....                                 | 5         |
| Firmware image naming convention.....                | 6         |
| FortiAnalyzer VM firmware.....                       | 7         |
| SNMP MIB download .....                              | 7         |
| Build numbers.....                                   | 7         |
| Firmware upgrade and support information .....       | 9         |
| <b>Upgrade Information .....</b>                     | <b>13</b> |
| Upgrading from FortiAnalyzer v5.0.6 or earlier ..... | 13        |
| Firmware upgrade steps .....                         | 13        |
| Distributed upgrades .....                           | 18        |
| Downgrading to previous versions .....               | 18        |

# Change Log

| Date       | Change Description |
|------------|--------------------|
| 2014-06-27 | Initial release.   |
|            |                    |
|            |                    |

# FortiAnalyzer Firmware

This document provides an overview of FortiAnalyzer firmware and highlights general information you should be aware of prior to upgrading your FortiAnalyzer device. This guide is intended to supplement the [FortiAnalyzer Release Notes](#) documentation.

The following topics are included in this section:

- [Best practices](#)
- [Firmware image naming convention](#)
- [FortiAnalyzer VM firmware](#)
- [SNMP MIB download](#)
- [Build numbers](#)
- [Firmware upgrade and support information](#)

## Best practices

Before any firmware upgrade complete the following:

- Download the FortiAnalyzer firmware image and Release Notes document from the [Fortinet Customer Service & Support](#) portal. Review the Release Notes including special notices, upgrade information, product integration and support, resolved and known issues.
- Prepare your FortiAnalyzer for upgrade and ensure your log devices are running the appropriate firmware versions as documented in the firmware Release Notes.
- Backup your configuration file and save this configuration file to your local computer. The device configuration file is saved with a `.dat` extension.



In VM environments, it is recommended that you clone the VM instance. In the event of an issue with the firmware upgrade, you can revert to the VM clone.



In VM environments, upgrade your VM server to latest stable update and patch release offered by the VM host server provider.

---

- Plan a maintenance window to complete the firmware upgrade. If possible, you may want to set up a test environment to ensure that the upgrade does not negatively impact your network or log devices.
- Once the upgrade is complete, test your FortiAnalyzer device to ensure that the upgrade was successful and that all log devices are listed.



Firmware best practice: Stay current on patch releases for your current major release. Only upgrade to a new major release or version when you are looking for specific functionality in the new major release or version. For more information, see the [FortiAnalyzer Release Notes](#) or contact Fortinet Technical Support.

## Firmware image naming convention

FortiAnalyzer firmware images in the [Fortinet Customer Service & Support](#) portal HTTPS and FTP Download tabs are organized by firmware version, major release, and patch release. The firmware images in the directories follow a specific naming convention and each firmware image is specific to the device model. For example, the FAZ\_300D-v500-build0310-FORTINET.out image found in the /FortiAnalyzer/v5.00/5.0/5.0.6 file folder is specific to the FortiAnalyzer 300D device model.

Figure 1 shows the /FortiAnalyzer/v5.00/5.0/5.0.6 file folder and highlights ❶ the firmware image for the FortiAnalyzer 300D and ❷ the location of the [FortiAnalyzer v5.0.6 Release Notes](#).

**Figure 1:** v5.0.6 file folder

Up to higher level directory

| Name  | Size     | Last Modified          |
|---|----------|------------------------|
| FAZ_1000B-v500-build0310-FORTINET.out                   | 29246 KB | 2014-03-18 6:04:00 PM  |
| FAZ_1000C-v500-build0310-FORTINET.out                   | 29158 KB | 2014-03-18 6:04:00 PM  |
| FAZ_1000D-v500-build0310-FORTINET.out                   | 30579 KB | 2014-03-18 6:05:00 PM  |
| FAZ_100C-v500-build0310-FORTINET.out                    | 27655 KB | 2014-03-18 6:05:00 PM  |
| FAZ_2000A-v500-build0310-FORTINET.out                   | 28853 KB | 2014-03-18 6:05:00 PM  |
| FAZ_2000B-v500-build0310-FORTINET.out                   | 29649 KB | 2014-03-18 6:05:00 PM  |
| FAZ_200D-v500-build0310-FORTINET.out                    | 29256 KB | 2014-03-18 6:05:00 PM  |
| FAZ_3000D-v500-build0310-FORTINET.out                   | 31153 KB | 2014-03-18 6:05:00 PM  |
| ❶  FAZ_300D-v500-build0310-FORTINET.out                 | 28408 KB | 2014-03-18 6:05:00 PM  |
| FAZ_4000A-v500-build0310-FORTINET.out                   | 29097 KB | 2014-03-18 6:05:00 PM  |
| FAZ_4000B-v500-build0310-FORTINET.out                   | 30024 KB | 2014-03-18 6:05:00 PM  |
| FAZ_400B-v500-build0310-FORTINET.out                    | 28584 KB | 2014-03-18 6:05:00 PM  |
| FAZ_400C-v500-build0310-FORTINET.out                    | 28320 KB | 2014-03-18 6:05:00 PM  |
| FAZ_VM32-v500-build0310-FORTINET.out                    | 29077 KB | 2014-03-18 6:06:00 PM  |
| FAZ_VM32-v500-build0310-FORTINET.out.vmdk               | 28924 KB | 2014-03-18 6:06:00 PM  |
| FAZ_VM32-v500-build0310-FORTINET.out.vmware.zip         | 28941 KB | 2014-03-18 6:06:00 PM  |
| FAZ_VM64-v500-build0310-FORTINET.out                    | 29806 KB | 2014-03-18 6:06:00 PM  |
| FAZ_VM64-v500-build0310-FORTINET.out.vmdk               | 29657 KB | 2014-03-18 6:06:00 PM  |
| FAZ_VM64-v500-build0310-FORTINET.out.vmware.zip         | 29673 KB | 2014-03-18 6:06:00 PM  |
| FAZ_VM64_HV-v500-build0310-FORTINET.out                 | 29876 KB | 2014-03-18 6:06:00 PM  |
| FAZ_VM64_HV-v500-build0310-FORTINET.out.hyperv.zip      | 29493 KB | 2014-03-18 6:06:00 PM  |
| FORTINET-FORTIMANAGER-FORTIANALYZER-MIB.mib             | 16 KB    | 2014-03-18 6:06:00 PM  |
| ❷  FortiAnalyzer-v5.0-Patch-Release-6-Release-Notes.pdf | 1096 KB  | 2014-04-15 10:36:00 PM |
| FortiAnalyzer-v5.0-Patch-Release-6-Upgrade-Guide.pdf    | 1221 KB  | 2014-04-15 10:37:00 PM |
| MIB   |          | 2014-02-06 3:11:00 AM  |
| md5sum.txt  | 2 KB     | 2014-03-18 6:06:00 PM  |
| mysql.schema  | 81 KB    | 2014-03-18 6:06:00 PM  |
| postgres.schema   | 78 KB    | 2014-03-18 6:06:00 PM  |

## FortiAnalyzer VM firmware

Fortinet provides FortiAnalyzer VM firmware images for both VMware ESX/ESXi and Microsoft Hyper-V Server virtualization environments.

### VMware ESX/ESXi

- FAZ\_VMxx-v500-buildxxxx-FORTINET.out: Download either the 32-bit or 64-bit firmware image to upgrade your existing FortiAnalyzer VM installation.
- FAZ\_VMxx-v500-buildxxxx-FORTINET.out.ovf.zip: Download either the 32-bit or 64-bit package for new FortiAnalyzer VM installations. The package contains a deployable Open Virtualization Format (OVF) virtual machine package for VMware ESX/ESXi installations and the faz.vmdk and datadrive.vmdk virtual machine disk format files.

### Microsoft Hyper-V Server

- FAZ\_VM64\_HV-v500-buildxxxx-FORTINET.out: Download the firmware image to upgrade your existing FortiAnalyzer VM installation.
- FAZ\_VM64\_HV-v500-buildxxxx-FORTINET.out.hyperv.zip: Download the package for a new FortiAnalyzer VM installation. This package contains a Virtual Hard Disk (VHD) file for Microsoft Hyper-V Server.

For more information see the FortiAnalyzer product data sheet available on the Fortinet web site, <http://www.fortinet.com/products/fortianalyzer/virtualappliances.html>.

## SNMP MIB download

You can download the *FORTINET-FORTIMANAGER-FORTIANALYZER.mib* MIB file in the firmware image file folder. The Fortinet Core MIB file is located in the main FortiAnalyzer v5.00 file folder.

## Build numbers

FortiAnalyzer firmware images are generally documented as a three-digit build number. New FortiAnalyzer models may be released on a special branch based off of the regular FortiAnalyzer firmware release. As such, the build number found in the *System Settings > Dashboard, System Information* widget and the output from the `get system status` CLI command displays this four-digit special build number as the build number.

To confirm that you are running the proper build, the output from the `get system status` CLI command has a `Branch point:` field that displays the regular three-digit build number.

The following examples provide the output from the `get system status` CLI command for both a regular firmware release and a new model firmware release.

### Example 1: Regular firmware release

```
Platform Type : FAZ2000A
Version : v5.0-build0232 130328 (GA Patch 4)
Serial Number : FLG-2K3F08000000
BIOS version : 04000001
Hostname : FortiAnalyzer-2000A
Max Number of Admin Domains : 2000
Admin Domain Configuration : Enabled
FIPS Mode : Disabled
Branch Point : 232
```

**Release Version Information : (GA Patch 4)**

Current Time : Wed Sep 13 14:20:53 PDT 2013  
Daylight Time Saving : Yes  
Time Zone : (GMT-8:00)Pacific Time(US&Canada)

Disk Usage : Free 1825.27GB, Total 1831.40GB  
RAID Level: Raid-5  
RAID Status: OK  
RAID Size: 1862GB

Disk 1: OK Used 465GB  
Disk 2: OK Used 465GB  
Disk 3: OK Used 465GB  
Disk 4: OK Used 465GB  
Disk 5: OK Not-Used 465GB  
Disk 6: OK Used 465GB

**Example 2: New model firmware release**

Platform Type : FAZ300D

**Version : v5.0-build4015 130416 (GA)**

Serial Number : FL300D3M000000000

BIOS version : 00010001

System Part-Number : P13424-01

Hostname : FAZ300D

Max Number of Admin Domains : 175

Admin Domain Configuration : Disabled

FIPS Mode : Disabled

**Branch Point : 151**

**Release Version Information : (GA)**

Current Time : Tue Apr 23 15:09:43 PDT 2013  
Daylight Time Saving : Yes  
Time Zone : (GMT-8:00)Pacific Time(US&Canada)

Disk Usage : Free 1831.09GB, Total 1833.78GB  
RAID Level: Raid-1  
RAID Status: OK  
RAID Size: 1953GB

Disk 1: OK Used 1953GB  
Disk 2: OK Used 1953GB



## Firmware upgrade and support information

The following table is for reference only. Review the applicable [FortiAnalyzer Releases Notes](#) prior to upgrading your FortiAnalyzer system.



The following table uses the naming convention '4.3.7', where the first digit reflects the version, the second digit reflects the major release, and the third digit reflects the patch release. For example, 4.3.7 is v4.0 MR3 Patch Release 7.

**Table 1:** FortiAnalyzer upgrade and support information

| FortiAnalyzer Firmware Version  | Build Number | Upgrade From            | FortiOS Version Support                                     |
|---|--------------|-------------------------|---|
| <b>FortiAnalyzer 5.0</b>  |              |                         |   |
| 5.0.7<br>Release Date: 2014-06-27   | 0321         | 5.0.6                   | 5.2.0<br>5.0.0 to 5.0.7<br>4.3.2 or later<br>4.2.0 or later |
| FortiAnalyzer 5.0.7 is available for the following models: FAZ-100C, FAZ-200D, FAZ-300D, FAZ-400B, FAZ-400C, FAZ-1000B, FAZ-1000C, FAZ-1000D, FAZ-2000A, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3500E, FAZ-4000A, FAZ-4000B, FAZ-VM32, FAZ-VM64, and FAZ-VM64-HV.   |              |                         |   |
| 5.0.6<br>Release Date: 2014-02-05   | 0310         | 5.0.5<br>4.3.7 or later | 5.0.0 to 5.0.7<br>4.3.2 or later<br>4.2.0 or later          |
| FortiAnalyzer 5.0.6 is available for the following models: FAZ-100C, FAZ-200D, FAZ-300D, FAZ-400B, FAZ-400C, FAZ-1000B, FAZ-1000C, FAZ-1000D, FAZ-2000A, FAZ-2000B, FAZ-3000D, FAZ-4000A, FAZ-4000B, FAZ-VM32, FAZ-VM64, and FAZ-VM64-HV.<br><br>FAZ-3000E is released on special build 4047.<br>FAZ-3500E is released on special build 4031. |              |                         |   |
| 5.0.5<br>Release Date: 2013-11-08   | 0266         | 5.0.4<br>4.3.7          | 5.0.0 to 5.0.4<br>4.3.2 or later<br>4.2.0 or later          |
| FortiAnalyzer 5.0.5 is available for the following models: FAZ-100C, FAZ-200D, FAZ-300D, FAZ-400B, FAZ-400C, FAZ-1000B, FAZ-1000C, FAZ-1000D, FAZ-2000A, FAZ-2000B, FAZ-3000D, FAZ-4000A, FAZ-4000B, FAZ-VM32, FAZ-VM64, and FAZ-VM64-HV.   |              |                         |   |
| 5.0.4<br>Release Date: 2013-09-13   | 0232         | 5.0.3                   | 5.0.0 to 5.0.4<br>4.3.2 or later<br>4.2.0 or later          |
| FortiAnalyzer 5.0.4 is available for the following models: FAZ-100C, FAZ-200D, FAZ-300D, FAZ-400B, FAZ-400C, FAZ-1000B, FAZ-1000C, FAZ-2000A, FAZ-2000B, FAZ-3000D, FAZ-4000A, FAZ-4000B, FAZ-VM32, FAZ-VM64, and FAZ-VM64-HV.  |              |                         |   |
| 5.0.3<br>Release Date: 2013-07-10   | 0200         | 5.0.1 or 5.0.2          | 5.0.0 to 5.0.3<br>4.3.2 or later<br>4.2.0 or later          |

**Table 1:** FortiAnalyzer upgrade and support information (continued)

| FortiAnalyzer Firmware Version   | Build Number | Upgrade From   | FortiOS Version Support                             |
|--|--------------|--|---|
| <p>FortiAnalyzer 5.0.3 is available for the following models: FAZ-100C, FAZ-200D, FAZ-300D, FAZ-400B, FAZ-400C, FAZ-1000B, FAZ-1000C, FAZ-2000A, FAZ-2000B, FAZ-4000A, FAZ-4000B, FAZ-VM32, FAZ-VM64, and FAZ-VM64-HV.</p> <p>FAZ-VM64-HV is released on the regular build.<br/>FAZ-1000D is released on special build 4024.</p> |              |  |   |
| 5.0.2<br>Release Date: 2013-03-28  | 0151         | 5.0.1  | 5.0.0 to 5.0.2<br>4.3.2 or later<br>4.2.0 or later  |
| <p>FortiAnalyzer 5.0.2 is available for the following models: FAZ-100C, FAZ-200D, FAZ-300D, FAZ-400B, FAZ-400C, FAZ-1000B, FAZ-1000C, FAZ-2000A, FAZ-2000B, FAZ-4000A, FAZ-4000B, FAZ-VM32, and FAZ-VM64.</p> <p>The FAZ-300D is released on special build 4018.<br/>The FAZ-3000D is released on special build 4014.</p>        |              |  |   |
| 5.0.1<br>Release Date: 2012-11-21  | 0087         | 4.3.5 or later   | 5.0.0 and 5.0.1<br>4.3.1 or later<br>4.2.0 or later |
| <p>FortiAnalyzer 5.0.1 is available for the following models: FAZ-100C, FAZ-200D, FAZ-400B, FAZ-400C, FAZ-1000B, FAZ-1000C, FAZ-2000A, FAZ-2000B, FAZ-4000A, FAZ-4000B, FAZ-VM32, and FAZ-VM64.</p> <p>The FAZ-300D is released on special build 4008.</p>   |              |  |   |
| 5.0.0<br>Release Date: 2012-11-01  | 0076         | Note: This image was removed from the <a href="#">Customer Service &amp; Support</a> portal. For more information, see the <a href="#">Customer Support Bulletin</a> in the image directory. |   |
| FortiAnalyzer 4.3  |              |  |   |
| 4.3.8<br>Release Date: 2013-11-26  | 0719         | 4.3.5 or later<br>4.2.6  | 4.3.0 or later<br>4.2.0 or later                    |
| <p>FortiAnalyzer 4.3.8 is available for the following models: FAZ-100B, FAZ-100C, FAZ-200D, FAZ-400B, FAZ-400C, FAZ-800, FAZ-800B, FAZ-1000B, FAZ-1000C, FAZ-2000, FAZ-2000A, FAZ-2000B, FAZ-4000, FAZ-4000A, FAZ-4000B, FAZ-VM32, and FAZ-VM64.</p>   |              |  |   |
| 4.3.7<br>Release Date: 2013-04-04  | 0705         | 4.3.5 or later<br>4.2.6  | 4.3.0 or later<br>4.2.0 or later                    |
| <p>FortiAnalyzer 4.3.7 is available for the following models: FAZ-100B, FAZ-100C, FAZ-200D, FAZ-400B, FAZ-400C, FAZ-800, FAZ-800B, FAZ-1000B, FAZ-1000C, FAZ-2000, FAZ-2000A, FAZ-2000B, FAZ-4000, FAZ-4000A, FAZ-4000B, FAZ-VM32, and FAZ-VM64.</p>   |              |  |   |
| 4.3.6<br>Release Date: 2012-12-05  | 0691         | 4.3.5<br>4.2.6   | 4.3.0 or later<br>4.2.0 or later                    |
| <p>FortiAnalyzer 4.3.6 is available for the following models: FAZ-100B, FAZ-100C, FAZ-200D, FAZ-400B, FAZ-400C, FAZ-800, FAZ-800B, FAZ-1000B, FAZ-1000C, FAZ-2000, FAZ-2000A, FAZ-2000B, FAZ-4000, FAZ-4000A, FAZ-4000B, FAZ-VM32, and FAZ-VM64.</p>   |              |  |   |

**Table 1:** FortiAnalyzer upgrade and support information (continued)

| FortiAnalyzer Firmware Version   | Build Number | Upgrade From            | FortiOS Version Support          |
|--|--------------|-------------------------|----------------------------------|
| 4.3.5<br>Release Date: 2012-07-24  | 0680         | 4.3.3 or later<br>4.2.6 | 4.3.0 or later<br>4.2.0 or later |
| FortiAnalyzer 4.3.5 is available for the following models: FAZ-100B, FAZ-100C, FAZ-400B, FAZ-400C, FAZ-800, FAZ-800B, FAZ-1000B, FAZ-1000C, FAZ-2000, FAZ-2000A, FAZ-2000B, FAZ-4000, FAZ-4000A, FAZ-4000B, FAZ-VM32, and FAZ-VM64.<br>Note: There is no image available for the FAZ-200D.       |              |                         |                                  |
| 4.3.4<br>Release Date: 2012-07-18  | 0679         | 4.3.3<br>4.2.6          | 4.3.0 or later<br>4.2.0 or later |
| FortiAnalyzer 4.3.4 is available for the following models: FAZ-100B, FAZ-100C, FAZ-400B, FAZ-400C, FAZ-800, FAZ-800B, FAZ-1000B, FAZ-1000C, FAZ-2000, FAZ-2000A, FAZ-2000B, FAZ-4000, FAZ-4000A, FAZ-4000B, FAZ-VM32, and FAZ-VM64.<br>Note: There is no image available for the FAZ-200D.       |              |                         |                                  |
| 4.3.3<br>Release Date: 2012-05-15  | 0654         | 4.3.2<br>4.2.6          | 4.3.0 or later<br>4.2.0 or later |
| FortiAnalyzer 4.3.3 is available for the following models: FAZ-100B, FAZ-100C, FAZ-200D, FAZ-400B, FAZ-400C, FAZ-800, FAZ-800B, FAZ-1000B, FAZ-1000C, FAZ-2000, FAZ-2000A, FAZ-2000B, FAZ-4000, FAZ-4000A, FAZ-4000B, FAZ-VM32, and FAZ-VM64.<br>The FAZ-200D is released on special build 4010. |              |                         |                                  |
| 4.3.2<br>Release Date: 2012-03-19  | 0632         | 4.3.1<br>4.2.5 or later | 4.3.0 or later<br>4.2.0 or later |
| FortiAnalyzer 4.3.2 is available for the following models: FAZ-100B, FAZ-100C, FAZ-400B, FAZ-400C, FAZ-800, FAZ-800B, FAZ-1000B, FAZ-1000C, FAZ-2000, FAZ-2000A, FAZ-2000B, FAZ-4000, FAZ-4000A, FAZ-4000B, FAZ-VM32, and FAZ-VM64.<br>The FAZ-400C is released on special build 4006.           |              |                         |                                  |
| 4.3.1<br>Release Date: 2011-10-06  | 0552         | 4.3.0<br>4.2.4 or later | 4.3.0 or later<br>4.2.0 or later |
| FortiAnalyzer 4.3.1 is available for the following models: FAZ-100B, FAZ-100C, FAZ-400B, FAZ-800, FAZ-800B, FAZ-1000B, FAZ-1000C, FAZ-2000, FAZ-2000A, FAZ-2000B, FAZ-4000, FAZ-4000A, FAZ-4000B, and FAZ-VM.  |              |                         |                                  |
| 4.3.0<br>Release Date: 2011-06-30  | 0513         | 4.2.4 or later          | 4.3.0 or later                   |
| FortiAnalyzer 4.3.0 is available for the following models: FAZ-100B, FAZ-100C, FAZ-400B, FAZ-800, FAZ-800B, FAZ-1000B, FAZ-1000C, FAZ-2000, FAZ-2000A, FAZ-2000B, FAZ-4000, FAZ-4000A, and FAZ-4000B.<br>Note: There is no image available for the FAZ-VM.                                       |              |                         |                                  |
| <b>FortiAnalyzer 4.2 is no longer supported (EOS) as of April 07, 2013.</b>  |              |                         |                                  |



Upon upgrading to FortiAnalyzer v5.0 Patch Release 1 or later, the system automatically begins converting the v4.0 MR3 logs, and inserts them into the SQL database. An icon appears at the top right corner after login to the Web-based Manager next to the logout and help buttons. This pops-up a small window displaying the progress. The time required depends on the size of the database.

---



Upgrading a FortiAnalyzer VM device from v4.0 MR3 Patch 6 or later to v5.0 Patch Release 1 or later is supported. The old VM license is converted into the new VM stackable license model. New VM installations running v5.0 Patch Release 1 or later can be deployed with the `.ovf` (VMware ESX/ESXi) or `.vhd` (Microsoft Hyper-V) file and application of either an old v4.0 MR3 or new v5.0 license.

---



FortiGate, FortiCarrier, FortiMail, FortiWeb, and syslog devices are supported in FortiAnalyzer v5.0 Patch Release 7. Other devices are not yet supported in FortiAnalyzer v5.0. For more information, see the [FortiAnalyzer v5.0.7 Release Notes](#).

---

# Upgrade Information

This section explains how to properly upgrade to FortiAnalyzer v5.0.7. The following topics are included in this section:

- [Upgrading from FortiAnalyzer v5.0.6 or earlier](#)
- [Firmware upgrade steps](#)
- [Distributed upgrades](#)
- [Downgrading to previous versions](#)

## Upgrading from FortiAnalyzer v5.0.6 or earlier

FortiAnalyzer v5.0.7 has re-sized the flash partition storing system firmware. In order to accommodate the re-sizing, you **MUST** upgrade to FortiAnalyzer v5.0.6 first. The secondary firmware and System Settings stored in the partition will be lost after upgrade. Please reconfigure System Settings as needed.

In VM environments, you will need to change the hard disk provisioned size to 513MB or more before powering on the FortiAnalyzer VM.



Upgrading your FortiAnalyzer 400B to v5.0.7 requires you to use an interim step. You **MUST** upgrade to the image named *FAZ\_400B-v500-FORTINET\_UpgradeThisBuildFirst.out* before upgrading to regular v5.0.7 image. The upgrade path looks like this:

*v5.0.6 or earlier > FAZ\_400B-v500-FORTINET\_UpgradeThisBuildFirst.out > v5.0.7*



Please upgrade your FortiAnalyzer 100C, 2000A, or 4000A via the Web-based Manager or command line interface. Upgrade via TFTP from BIOS is not supported for these models.

## Firmware upgrade steps

The following table lists the firmware upgrade steps.

**Table 2:** Upgrade steps

|               |  |
|---------------|--|
| <b>Step 1</b> | Prepare your FortiAnalyzer for upgrade.  |
| <b>Step 2</b> | Backup your FortiAnalyzer system configuration. For FortiAnalyzer VM, clone the VM instance. |
| <b>Step 3</b> | For FortiAnalyzer VM, change the hard disk provisioned size.                                 |
| <b>Step 4</b> | Transfer the firmware image to your FortiAnalyzer device.                                    |
| <b>Step 5</b> | Log into your FortiAnalyzer Web-based Manager to verify the upgrade was successful.          |

## Step 1: Prepare your FortiAnalyzer for upgrade

1. Make sure all log devices are running the supported firmware version as stated in the Release Notes.
2. Log in to the Fortinet Customer Service & Support portal at <https://support.fortinet.com>.
3. Select *Download* from the toolbar and select *Firmware Images* from the drop-down list.

Figure 2: Firmware image page

**FORTINET**  
CUSTOMER SERVICE & SUPPORT

Home Asset Assistance **Download** Feedback

FortiGuard Service Updates  
**Firmware Images**  
Firmware Image Checksums  
HQIP Images

**Firmware Images**  
Fortinet Firmware Images And Software Releases

**Firmware Images**

Welcome to the Firmware Images download center for Fortinet's extensive line of security solutions.

Select Product

FortiAnalyzer

**Release Notes** HTTPS Download FTP Download

Below is a series of periodic updates and advisories about the current and upcoming firmware and/or software releases for Fortinet products, please read the associated release notes for further details. All dates listed here are estimated and may be subject to change without notice.

Please read the release notes carefully

| FortiAnalyzer 5.0 | Description              | Notes                      |
|-------------------|--------------------------|----------------------------|
| 5.0.6 Build 0310  | Latest 5.0 Patch Release | Released 5 February 2014   |
| 5.0.5 Build 0266  | Latest 5.0 Patch Release | Released 9 November 2013   |
| 5.0.4 Build 0232  | Latest 5.0 Patch Release | Released 13 September 2013 |
| 5.0.3 Build 0200  | Latest 5.0 Patch Release | Released 10 July 2013      |

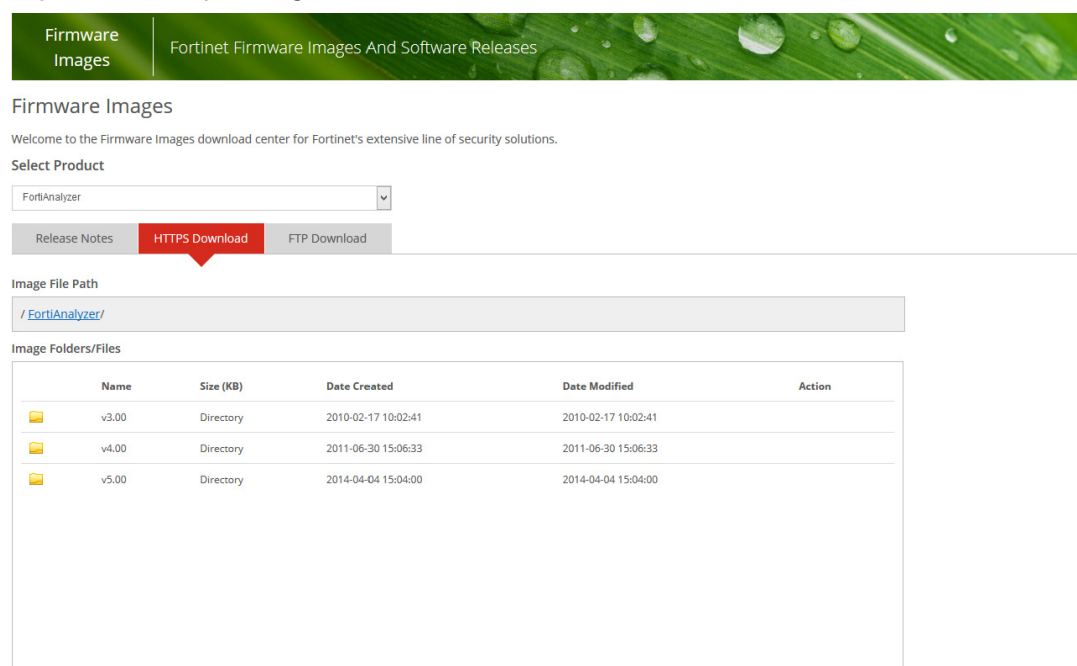
| FortiAnalyzer 4.0      | Description              | Notes                     |
|------------------------|--------------------------|---------------------------|
| MR3 Patch 8 Build 0719 | Latest MR3 Patch Release | Released 27 November 2013 |

You can also access the latest Firmware releases by adding our RSS feed, simply copy the URL below and follow your RSS reader's instructions for adding a new RSS feed.

**RSS Feed**

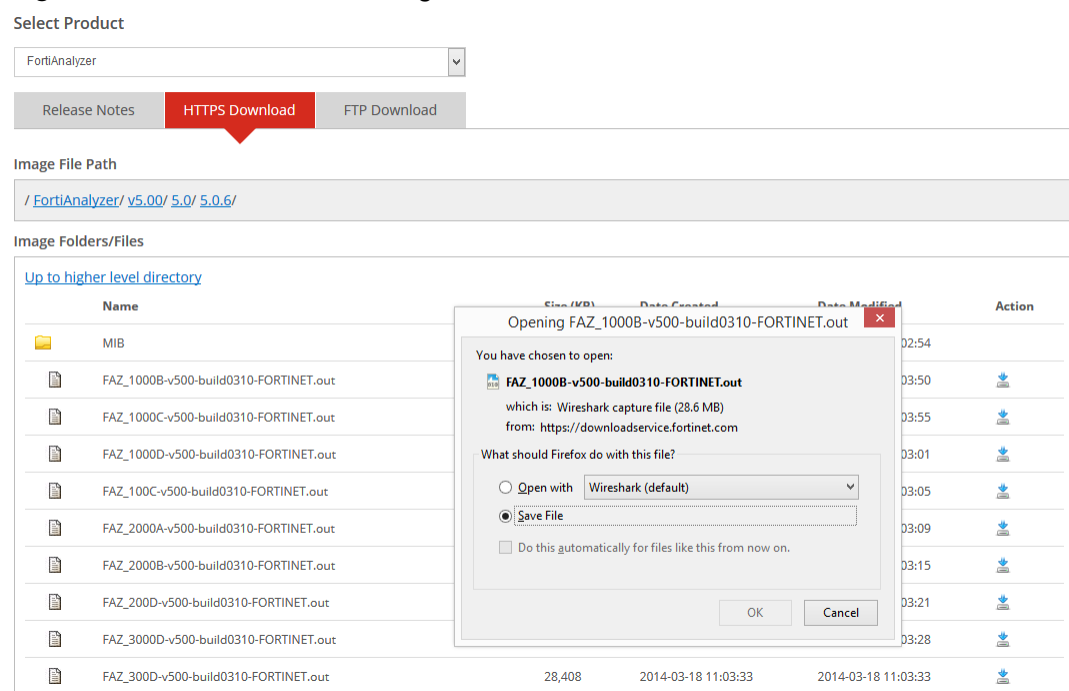
4. Select *FortiAnalyzer* from the drop-down list and select the *HTTPS Download* tab. Alternatively, you can select *FTP Download*. FTP is not an encrypted file transferring protocol and HTTPS download is recommended.
- The image folders are displayed.

**Figure 3:** Example image folders



5. Browse to the appropriate file folder to download the firmware image (.out) and Release Notes document.

**Figure 4:** Download firmware image



6. Select an image in the list to download the firmware image to your management computer.
7. To verify the integrity of the download, select *Download* from the toolbar and select *Firmware Image Checksums* from the drop-down list.

**Figure 5:** Firmware image checksums page

**Firmware Image Checksums**

The firmware image checksum is required when you install firmware images to Fortinet products. It is used by system to evaluate the firmware image. This information could be retrieved by providing firmware image file name in this page.

Image File Name:

FAZ\_VM64\_HV-v500-build0266-FORTINET.out

Get Checksum Code

Image File Name: FAZ\_VM64\_HV-v500-build0266-FORTINET.out  
Checksum Code: 3edd858ba9882cb425e8d2f5e7fc6ff3

8. Enter the file name and select *Get Checksum Code* to get the firmware image checksum code. Compare this checksum with the checksum of the firmware image.

## Step 2: Back up your FortiAnalyzer configuration

1. Go to *System Settings > Dashboard*.
2. Select *Backup* in the *System Information* widget.

**Figure 6:** System information widget

| System Information     |   |
|------------------------|---|
| Host Name              | FAZVM64 <a href="#">[Change]</a>  |
| Serial Number          | <a href="#">[View serial number details]</a>                                  |
| Platform Type          | FAZVM64   |
| System Time            | Thu Jun 26 13:31:47 PDT 2014 <a href="#">[Change]</a>                         |
| Firmware Version       | 4.0.0.0-140626133147-140626133147-140626133147 <a href="#">[Update]</a>       |
| System Configuration   | Last Backup: N/A <a href="#">[Backup]</a> <a href="#">[Restore]</a>           |
| Current Administrators | admin <a href="#">[Change Password]</a> / 1 in Total <a href="#">[Detail]</a> |
| Up Time                | 0 day 4 hours 25 minutes 33 seconds   |
| Administrative Domain  | Enabled <a href="#">[Disable]</a>   |
| Operation Mode         | Analyzer <a href="#">[Change]</a>   |

The *Backup* dialog box opens.

**Figure 7:** Backup dialog box

**Backup**

☒ Encryption

Password  (maximum length: 15)

Confirm Password  (maximum length: 15)

OK Cancel

3. Select the checkbox to encrypt the backup file and enter a password.



When selecting to encrypt the backup configuration file, the same password used to encrypt the file will be required to restore this backup file to the FortiAnalyzer device.



4. Select **OK** and save the backup file on your local computer.



Optionally, you can backup the configuration file to a FTP, SFTP, or SCP server using the following CLI command:

```
execute backup all-settings {ftp | sftp} <server IP address>
    <path/filename to the server> <user name on server> <password>
    [cryptpasswd]
execute backup all-settings scp <server IP address> <path/filename to
    the server> <user name on server> <SSH certificate> <crptpassrd>
```

For more information, see the [FortiAnalyzer CLI Reference](#).

5. In VM environments, it is recommended that you clone VM instance. In the event of an issue with the firmware upgrade, you can revert to the VM clone.

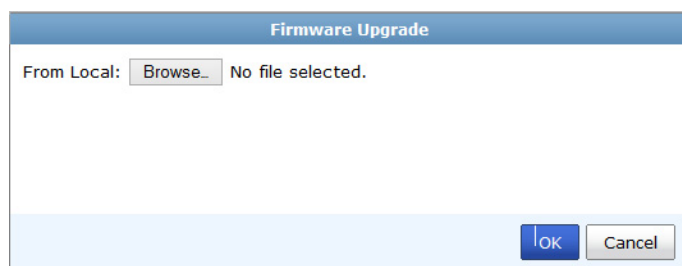
### Step 3: Change the FortiAnalyzer VM hard disk provisioned size

1. For VM environments, change the hard disk provisioned size to 513MB or more before upgrading your FortiAnalyzer VM.

### Step 4: Transfer the firmware image to your FortiAnalyzer device

1. Go to *System Settings > Dashboard*.
2. In the *System Information* widget, in the *Firmware Version* field, select *Update*. The *Firmware Upgrade* dialog box opens.

**Figure 8:** Firmware upgrade dialog box



3. Select *Browse* to locate the firmware image (.out file) that you downloaded from the [Fortinet Customer Service & Support](#) portal and select *Open*.
4. Select **OK** to continue with the upgrade. Your FortiAnalyzer will upload the firmware image and you will receive a confirmation message noting that the upgrade was successful.



Optionally, you can upgrade firmware stored on a FTP or TFTP server using the following CLI command:

```
exexecute restore image {ftp | tftp} <file path on the FTP server>
    <server IP address <user name on server> <password>
```

For more information, see the [FortiAnalyzer CLI Reference](#).

### Step 5: Verify the upgrade

1. Refresh the browser page and log back into the device.
2. Launch the *Device Manager* module and make sure that all formerly added log devices are still listed.
3. Launch the other functional modules and make sure they work properly.

## Distributed upgrades

For Collector/Analyzer architecture upgrades, Fortinet recommends upgrading the Analyzer first.



Upgrading the Collector first could impact the Analyzer's performance.

---

## Downgrading to previous versions

FortiAnalyzer does not provide a full downgrade path. You can downgrade to a previous FortiAnalyzer firmware release via the Web-based Manager or CLI, but doing so results in configuration loss. A system reset is required after the firmware downgrading process has completed. To reset the system, use the following CLI commands via a console port connection:

```
execute reset all-settings
execute format {disk | disk-ext4}
```

